UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,258	12/07/2004	Katsuhiro Nakai	2004_1946A	1207

513 7590 01/02/2009

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
01/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/517,258	NAKAI ET AL.	
	Examiner	Art Unit	
	CHINWENDU C. OKORONKWO	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 11/15/2006, the Examiner acknowledges the amendments made to the claims and have both considered and applied them to the claims.

Claims 1-18 are presented for examination.

Response to Remarks/Arguments

2. Applicant's arguments with respect to the rejection of the claims have been fully considered but they are not persuasive.

2.1 In response to Applicant argument that the Richards et al. reference does not teach or suggest a semiconductor integrated circuit device is operable to check or judge whether a rewrite program, which is secret information that is not leaked to a third party, stored in a RAM memory is correct or correctly stored, the Examiner respectfully disagrees citing column 6 lines 5-15, which recites, "because the data link is an open link and subject to third parties possibly intercepting or replacing applications being transmitted, security measures which authenticate the application itself, the application provider and the IC card must be used to ensure the integrity of the system." The disclosed integrity of the system is equated to the correct storage claimed and argued by the Applicant. Further the recitation of column 6 lines 52-63, "KTU contains information relating to the encryption of the AU 203 (the code and data of the application) which allows the IC card to decrypt the designated portions so that the

application and data can be accessed by the IC card but protects the data during transmission between the application provider and the IC card" reads upon the claimed and argued checking or judging if the storage was correct and reading only a specific portion of the rewrite program accordingly. Based on the above disclosure, the Examiner maintains that the Richards et al. reference does indeed disclose the argued and amended claim limitations as the disclosed security measures which authenticate the application and ensure the integrity of the system read upon the claimed checking/judging or determination of whether a rewrite program was stored in memory correctly.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

The term "correct" in claims 1, 2, 5, 7, 8 and 16 is a relative term which renders the claim indefinite. The term "correct" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-18 are rejected under 35 U.S.C. 102(b) as being disclosed by Richards et al. (U.S. Patent No. 6,230,267).

Regarding claims 1, 7-8, 14, 16 and 18, Richards et al., discloses a semiconductor integrated circuit device having a second storage means in a semiconductor integrated circuit:

- in which a program that makes an arithmetic processing unit in the semiconductor integrated circuit perform an operation of processing contents is rewritably stored (5:61-66 – "secure method for loading applications" is equated to the claimed rewritably stored contents), and performing rewriting of the program stored in the second storage means using a first storage means in which a rewrite program for rewriting is stored, which rewrite program makes the arithmetic processing unit perform an operation of processing the contents (Figure 1A and 5:65-67 and 6:1-3 – "application provider" (equated to the first storage means) "initiates an application loading process onto IC card 103" (equated to the second storage means) "… [t]he application provider 101 … desires to send and load an application to the IC card");
- wherein said second storage means has an externally readable area that can be read from the outside of the semiconductor integrated circuit, and

an externally unreadable area that cannot be read from the outside (Figure 1A elements 15-19) and

- after arbitrary data is stored in the externally readable area of the second storage means (5:51-61 – "data can be processed by the IC card 3"), the data is read to the outside of the semiconductor integrated circuit to check whether the arbitrary data is the data as inputted (5:42-49 – "transmitting entity then verifies the public key certificate with public key of the CA 13 which is publicly available from the CA 9 and may be stored in the transmitting entity"), and thereafter, the rewrite program read from the first storage means is stored in the externally unreadable area of the second storage means (5:51-61 – "data can be processed by the IC card 3. Only the IC card 3 has a copy of its private key so only the intended IC card can access the encrypted data. This ensures that third parties cannot access the encrypted data and correspondingly that only the intended IC card will be able to read and process the data").

Regarding claims 2 and 9, Richards et al., discloses semiconductor integrated circuit device having a second storage means in a semiconductor integrated circuit:

- in which a program that makes an arithmetic processing unit in the semiconductor integrated circuit perform an operation of processing contents is rewritably stored, and performing rewriting of the program

stored in the second storage means using a first storage means in which a rewrite program for rewriting is stored, which rewrite program makes the arithmetic processing unit perform an operation of processing the contents, said semiconductor integrated circuit device including:

- a control circuit for performing control so as to read only a specific portion of the rewrite program stored in the second storage means which is used for judging whether the rewrite program is correct or not (6:5-15 – "because the data link is an open link and subject to third parties possibly intercepting or replacing applications being transmitted, security measures which authenticate the application itself, the application provider and the IC card must be used to ensure the integrity of the system" and 6:52-63 – "KTU contains information relating to the encryption of the Au 203 (the code and data of the application) which allows the IC card to decrypt the designated portions so that the application and data can be accessed by the IC card but protects the data during transmission between the application provider and the IC card.")
- wherein said second storage means has an externally readable area that can be read from the outside of the semiconductor integrated circuit, and an externally unreadable area that cannot be read from the outside (Figure 2 and 6:34-42 – "Application Unit (AU) 203 … [which] contains the application code and data which are to stored on the IC card, some or all of which is encrypted to protect a secret portion or portions of the code

and/or data.") and after arbitrary data is stored in the externally readable area of the second storage means, the data is read to the outside of the semiconductor integrated circuit to check whether the arbitrary data is the data as inputted, and thereafter, the rewrite program read from the first storage means is stored in the externally unreadable area of the second storage means (Figure 1A elements 15-19 and 5:51-61 – "data can be processed by the IC card 3. Only the IC card 3 has a copy of its private key so only the intended IC card can access the encrypted data. This ensures that third parties cannot access the encrypted data and correspondingly that only the intended IC card will be able to read and process the data").

Regarding claims 3-4, 10 and 17, Richards et al., discloses a semiconductor integrated circuit device wherein said control circuit performs control so as to read only the rewrite program located in specific addresses of the second storage means (8:65-67 – "public key of an IC card is freely available to anyone and can be obtained from the card directly ... [whereas] only the intended IC card can use its secret key of the public/secret key pair … identify the encrypted portions of the application being loaded and use the keys to decrypt and recover the entire application and associate data. Because no other entity has the secret key of the IC card, the security and integrity of the [application] and data being

transmitted is ensured.").

Regarding claims 5 and 11, Richards et al., discloses semiconductor integrated circuit device having a second storage means in a semiconductor integrated circuit:

- in which a program that makes an arithmetic processing unit in the semiconductor integrated circuit perform an operation of processing contents is rewritably stored, and performing rewriting of the program stored in the second storage means using a first storage means in which a rewrite program for rewriting is stored, which rewrite program makes the arithmetic processing unit perform an operation of processing the contents (Figure 1A and 5:65-67 and 6:1-3 – "application provider" equated to the first storage means "initiates an application loading process onto IC card 103 ... [t]he application provider 101 ... desires to send and load an application to the IC card");
- wherein said rewrite program includes a program for executing a portion of the rewrite program after the rewriting and the portion of the rewrite program stored in the second storage means is executed (8:65-67 – "public key of an IC card is freely available to anyone and can be obtained from the card directly ... [whereas] only the intended IC card can use its secret key of the public/secret key pair ...[to] identify the encrypted portions of the application being loaded and use the keys to decrypt and

recover the entire application and associate data. Because no other entity has the secret key of the IC card, the security and integrity of the [application] and data being transmitted is ensured." And 9:28-31 – "feild allows the microprocessor on the IC card to know how large an area has been encrypted and when coupled with the start of the area, allows the IC card microprocessor to decrypt the correct portion")

Regarding claims 6 and 12-13, Richards et al., discloses a semiconductor integrated circuit device wherein the portion of the rewrite program to be executed is one for successively executing discontinuous program areas (Figure 2 and 6:34-42 – "Application Unit (AU) 203 ... [which] contains the application code and data which are to stored on the IC card, some or all of which is encrypted to protect a secret portion or portions of the code and/or data.")

Regarding claim 15, Richards et al., discloses semiconductor integrated circuit device as defined in claim 1 further including, in the semiconductor integrated circuit, a decryption means for decrypting the encrypted rewrite program; wherein, when the rewrite program stored in the first storage means has previously been encrypted, the decryption means decrypts the encrypted program, and stores the decrypted rewrite program in the second storage means (11:42-46 – "decrypts the identified portion with the identified decryption technique. This allows the IC card to have the decrypted portion of the AU which

it will stored in its EEPROM once all the encrypted portions have been decrypted.").

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHINWENDU C. OKORONKWO whose telephone number is (571)272-2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436